US Army Corps
of Engineers

Electronic Signature
for
Windows 95/NT

(WinSig)

Users Guide

CEFMS

March 28, 2001

Corps of Engineers Financial Management System

Electronic Signature
For Windows 95/NT
(WinSig)
Users Guide

WINSIG USERS GUIDE

TABLE OF CONTENTS

PAGE

WINSIG USERS GUIDE

SECTION 1.0 GENERAL

1.1 Introduction.

The Corps of Engineers Financial Management System (CEFMS) provides the capability to electronically sign documents. The electronic signature generated by the system is a replacement for a handwritten signature. An electronic signature provides assurance that an authorized person signed a document and that the document was not altered after it was signed. Hardcopy documents can be altered without detection and handwritten signatures can be forged. With electronic signatures, these alterations will be detected. Electronic Signatures will reduce the amount of paper that must be routed. Documents can be reviewed on screen and signatures verified using the Electronic Signature System (ESS).

An Electronic Signature, or Message Authentication Code (MAC), is a cryptographic checksum calculated by a cryptographic algorithm, based on the Digital Encryption Standard. This algorithm is stored in firmware which resides in the user’s PC. The information that must be supplied to the cryptographic module so that a MAC can be generated include:

- A secret key belonging to the person signing or MACing the data. This person is the user.

- A secret key belonging to the person allowing the user to electronically sign data. This person is the Security Administrator (SA).

- The data to be MACed.

Reference the MAC Cross Reference Guide for a detailed explanation of the MACing procedure.

The secret keys are resident on each SA and user smartcard and in the smartcard database at each Key Translation Center (KTC). A smartcard (also referred to as "token") is similar to a credit card but contains a complete computer resident in chip form. The signing process generates a MAC and an encryption key. Please note that the data is not encrypted. The encryption key is used in the verification process and is not an encrypted form of the data. At any point in time, the MAC may be verified. The verification process ensures that none of the data associated with the MAC has changed. The verification process also requires the secret keys of an SA and user. The SA and user that request to verify a MAC do not have access to the secret keys of the SA and user which generated the MAC. This is where key translation comes into the Electronic Signature process. The IDs of the SA and user that were used to generate the MAC plus the IDs of the SA and user wishing to verify the MAC along with the original encryption key must be sent to the KTC. If the information received by the KTC is valid, the KTC will generate a verification key based upon the received information and send the verification key back to the SA and user wishing to verify the MAC. The process of generating a verification key is called *key translation*. The verification key, along with the secret keys of the SA and user wishing to verify the MAC and the data are input to the cryptographic module which results in the generation of another MAC. If this new MAC and the original MAC are identical, the data has not changed. Different MACs indicate that the data has changed and the verification fails.

In addition to providing key translation services, the KTC provides the capability to:

- Create User Smartcards
- Create SA Smartcards
- Create District Security Officer (dSO) Smartcards
- Create Central Security Officer (cSO) Smartcards
- Transmit key information between KTCs electronically and on magnetic media

1.2 Explanation of WinSig.

The initial CEFMS electronic signature system was designed and implemented using the UNIX system standard-in and standard-out file descriptors to perform all communications between CEFMS (at the remote host) and the cryptographic module in each user's computer. This design was based on the domination of the DOS operating system, therefore, no other options were readily viable.

Due to technological changes, Microsoft Windows is rapidly becoming the operating system of choice. Microsoft Window's graphical interface and multitasking capabilities make it very appealing to computer users. To keep up with the needs of CEFMS users, the U.S. Army Corps of Engineers (USACE), determined that CEFMS should migrate to the Windows environment. In order to make this transition possible, the first step is to convert the electronic signature system since it is both DOS-based and terminal dependent. To facilitate this port, the electronic signature system has been rewritten to work in a Windows environment. The new software is called WinSig, and it provides the following benefits:

- Users are no longer bound by the limitations of DOS.

- Electronic signature is no longer dependent on a specific communications medium, therefore, allowing users a choice of terminal emulator. Any terminal emulator that can support CORP220 emulation can be used with WinSig.

- Portability of CEFMS to Windows will be minimal because WinSig already works in Windows. Only the user exit portion (the subsystem that actually talks to the database) will need to be ported from UNIX to Windows.

- The WinSig design makes the port to a database trigger-based electronic signature system easier and less time-consuming.

- WinSig is generic; making it easily integrated into other applications, like travel systems, or e-mail systems.

- Users can see, on their screen, a detailed list of all the data they are signing, and elect whether to sign it or not.

- Signature failure resolution is performed interactively, and the users can elect to re-sign a document while still in CEFMS.

- Communications hashing is no longer needed, since the users sign data visible on their screen. Elimination of communications hashing reduces the number of UNIX processes that were required and the increased communication traffic for KTC access.

- There is no longer a need for standalone resigning programs.

1.3 Hardware/Software Requirements.

The basic computer software and hardware required to run and use the WinSig suite include:

- A PC with one available ISA slot, capable of running Windows 95 or NT. **NOTE:** WinSig will not work on a Macintosh. WinSig may be used with a notebook computer with the Signet device, when the Signet driver for WinSig becomes available. If using the Signet device, one serial port is needed.

- Windows 95 or NT.

- Capability to access the CEFMS database via a telnet connection. Users wishing to use WinSig with a modem will need to use the Windows Dial-up Networking software, or a similar product.

- Cryptographic module and smartcard reader.

- WinSig.

- Activated Smartcard and personal identification number (PIN) for same.

- Users who will not be using the CEFMS electronic signature capabilities will still need to run WinSig with the NoBoard package, in order to be able to print and transfer files.

1.4 Installation Instructions.

WinSig is currently composed of three separate pieces of software: WinSig itself, the CEFMS package for WinSig, and the NoBoard package for WinSig. Use the following to determine what you need:

- All users need WinSig
- Users with a cryptographic module need the "CEFMS package for WinSig":
- Users without a cryptographic module need the "NoBoard package for WinSig"

To obtain the software, point your web browser to http://www.esig.com/cefms.html, and follow the download instructions there. It is best to download the software to a temporary location on your PC. When you have downloaded the software you need, you are ready to install.

***NOTE*: When installing the software on a new PC, WinSig must always be the first software installed, because the other packages install themselves relative to the WinSig installation directory.**

Each piece of the WinSig suite is in a single self-extracting executable. To begin the installation process, uncompress the executable by running it. Uncompressing the file will create a group of files in the download directory. To begin the installation, run the setup program (“SETUP.EXE”) created during the extraction. This will start an InstallShield setup. Please follow the instructions given in the setup process. It is recommended that only advanced users modify any of the default settings in the Setup process. At the end of the Setup process, a prompt to “Launch program file” is displayed. *Always* select the box next to this prompt before exiting the Setup program.

When finished with the Setup processes for all the software you need, run the WinSig Package Manager (found on the Start menu). In the Package Manager, select the appropriate package for use by checking the box next to its name in the “Available packages” list. *WinSig will not use a package unless it is selected for use and is configured properly.*

1.4.1 CEFMS Package for WinSig Configuration.

To configure the CEFMS package for WinSig, click the “Configure” button in the Package Manager. In the “CEFMS Package Configuration Central” utility, enter the following values: If your CEFMS host machine is located in Vicksburg, MS (i.e., a “cpc” machine), then your Primary KTC is “tk4.usace.army.mil” and your Secondary KTC is “tk3.usace.army.mil” (please do not put quotes when entering the KTC names). If your CEFMS host machine is located in Portland, OR (i.e., a “wpc” machine), then your Primary KTC is “tk3.usace.army.mil”, and your Secondary KTC is “tk4.usace.army.mil” (please do not put quotes when you are entering the KTC names).

If an Argus/300 cryptographic module is used in your PC, then your Cryptographic module DLL should be "ARGUS300.DLL", which can be found in the “\PACKAGES\CEFMSPKG” subdirectory off the WinSig base directory (“C:\CEFMS\WINSIG”, if you took the defaults on the install). Be sure to leave out the quotes when entering the value for the cryptographic DLL. If you use the “Browse for DLL” button, you should be able to find the DLL with no problems.

Click the “Configure DLL...” button in the CEFMS Package Configuration Central to configure the cryptographic DLL. In the DLL configuration window, click the

“Search for hardware...” button to set-up the proper address for your cryptographic module, or WinSig will not work properly.

Once the utility has found your hardware, click the “Ok” button to return to the CEFMS Package Configuration Central utility. If the software cannot find your cryptographic module’s hardware address, please contact your local support. When you have entered all the values for the configuration utility, click the “Ok” button to save the changes and exit the configuration utility.

1.4.2 NoBoard Package for WinSig Configuration.

To configure the NoBoard package for WinSig, click the “Configure” button in the Package Manager. In the “NoBoard Package Configuration Central” utility, enter the following values: If your CEFMS host machine is located in Vicksburg, MS (i.e., a “cpc” machine) then your Primary KTC is “tk4.usace.army.mil”, and your Secondary KTC is “tk3.usace.army.mil” (please do not put quotes when entering the KTC names). If your CEFMS host machine is located in Portland, OR (i.e., a “wpc” machine), then your Primary KTC is “tk3.usace.army.mil”, and your Secondary KTC is “tk4.usace.army.mil” (please do not put quotes when entering the KTC names).

If you wish to go ahead and register yourself to WinSig, enter your CEAP logon ID in the appropriate box, and click the “Register now” button. This tells WinSig where you are located on the CEAP network. Click the “Done” button in the WinSig Package Manager to close it. WinSig is now ready to run.

1.5 Instructions on Using WinSig Features.

1.5.1 Starting WinSig.

The WinSig executable is located in the directory where you installed WinSig. If you took the installation defaults, that directory is C:\CEFMS\WINSIG. The WinSig executable is WINSIG.EXE. Additionally, if you took the installation defaults, a link to WinSig should also be in your computer’s Startup group, thereby starting WinSig each time you boot your PC.

1.5.2 User and Smartcard Registration.

With WinSig, CEFMS must know the IP address of the PC that a user is using to access CEFMS. To provide that information to CEFMS, a user must register their smartcard before accessing CEFMS. Registering a smartcard is accomplished by simply inserting your smartcard into the smartcard reader attached to the PC that you will use to access CEFMS. Nothing will prompt you to do this. When the smartcard is inserted into the card reader a window will appear announcing that the smartcard is beging registered. If this is the first time that you have registered your card another window will pop up asking that you enter your UNIX logon ID. It is important that you enter the ID correctly. Your UNIX logon ID is the same as your “CEAP ID” and is in the form of “u4rmfsrk”. Once the ID has been entered, both windows will close in a second or two. When the registration widows have closed, your card has been registered. You are now ready to use CEFMS. Once the WinSig registration system knows your ID, you will not be prompted to enter it upon successive registrations.

Users using the NoBoard package for WinSig should register themselves during the installation and configuration of the software. Should a NoBoard user ever need to re-register (i.e., due to an IP address change), the WMANREG.EXE program can be run to accomplish this. This program is located in the PACKAGES\NOBRDPKG\BIN directory off the WinSig base directory (usually C:\CEFMS\WINSIG).

NOTE: Any time a user’s IP address changes, that user needs to re-register to WinSig, either by inserting his smartcard (with the CEFMS package), or by running the WMANREG program from the startup menu (for NoBoard users). Several things can cause an IP address change: moving to another machine, the use of dynamic addressing (DHCP), or a system reboot. ***Failure by a user to re-register upon an IP address change will cause WinSig to work improperly.*** **For users with smartcards, it is recommended that you get into the practice of always inserting your smartcard before you enter CEFMS, to prevent these problems.**

If a user tries to enter CEFMS and CEFMS locks up or the user gets into CEFMS with esig errors, most likely he/she is not registered properly.

If a user moves from one machine to another, he/she will need to re-register.

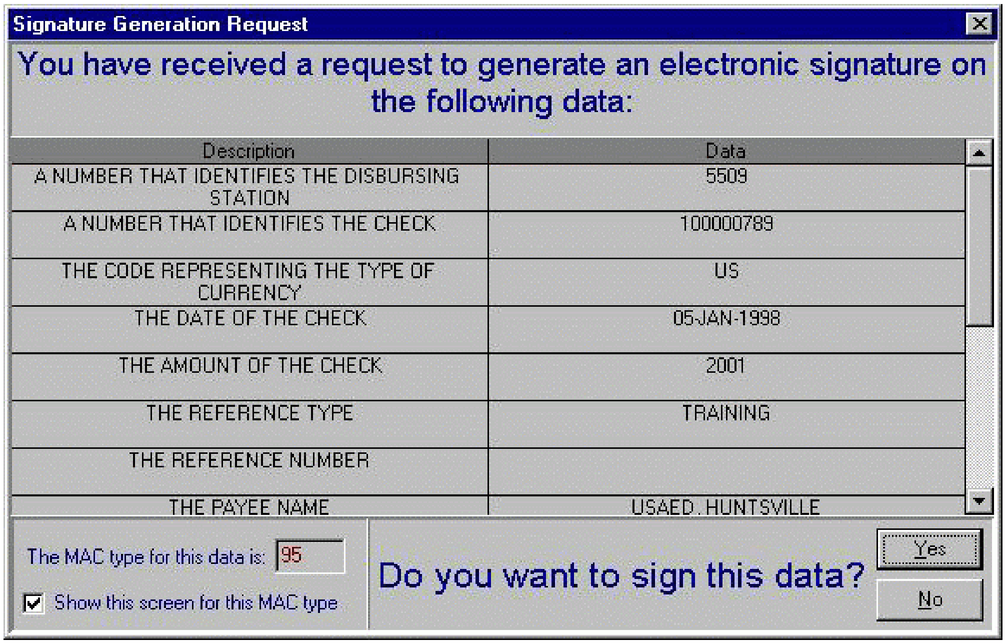
If the PC IP address changes (usually do to dynamic addressing), the user must re-register.

Several users can share a PC and be registered simultaneously to a PC; however, a user must re-register when using another PC.

The user ID is used by the registry to link a particular CEAP ID with a smartcard (if applicable) and an IP address. WinSig uses ports 2400-2405, and the registry system uses 2198-2199.

1.5.3 Signature Generation.

With WinSig, no electronic signature will be generated without the express consent of the user generating the signature. Any time you need to sign some data in CEFMS, you will see a window like the one shown below.



Signature Generation Request

You have received a request to generate an electronic signature on the following data:

Description	Data
A NUMBER THAT IDENTIFIES THE DISBURSING STATION	5509
A NUMBER THAT IDENTIFIES THE CHECK	100000789
THE CODE REPRESENTING THE TYPE OF CURRENCY	US
THE DATE OF THE CHECK	05-JAN-1998
THE AMOUNT OF THE CHECK	2001
THE REFERENCE TYPE	TRAINING
THE REFERENCE NUMBER	
THE PAYEE NAME	USAED, HUNTSVILLE

The MAC type for this data is: 95

☑ Show this screen for this MAC type

Do you want to sign this data?

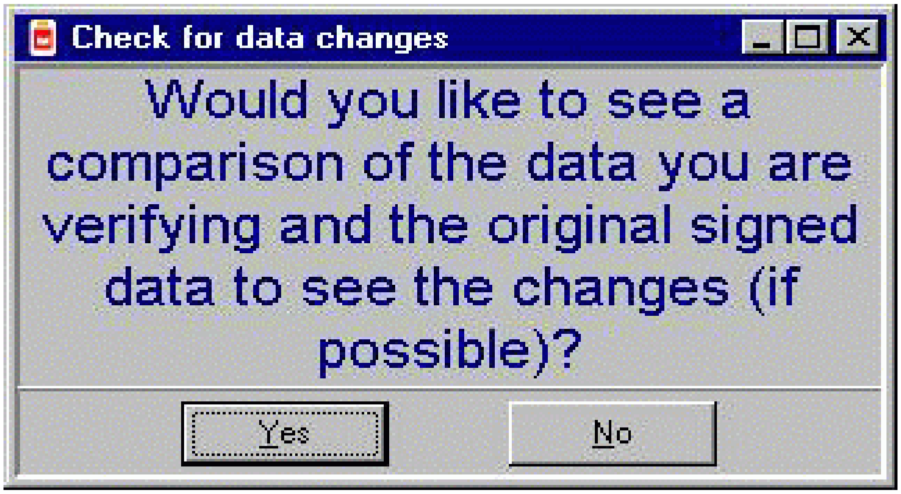
All data for a signature is shown in the window, and the scroll bar can be used to navigate the data. To sign the shown data, click the “Yes” button. To decline signing, click “No”. For users signing several documents of the same type over and over (for example, people in disbursing), the check box next to “Show this screen for this MAC type” can be unchecked. If the box is unchecked, the user will not be able to view the data before signing. This process is called *ignoring* a particular MAC type.

NOTE: If you ignore a particular MAC type, the window above will *not* be shown for that MAC. WinSig will assume on ignored MACs that you wish to generate the signature and will sign the received data without prompting you. The user is still responsible for the data being signed. Please do not fail to see the potential ramifications of ignoring a signature type.

If you ever want to remove the ignore on a particular MAC type, you can do so by clicking the “Ignores” button in the CEFMS Package for WinSig configuration utility and following the instructions you see there. To get to the configuration utility, run the WinSig Package Manager, select CEFMS, and click the configure button.

1.5.4 <u>Signature Verification</u>.

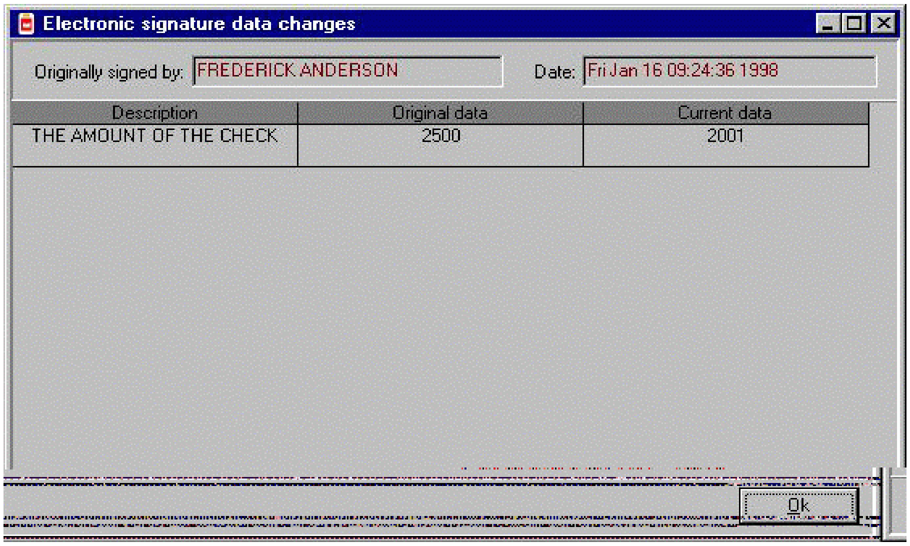
Signature verification in WinSig, for the most part, is like the signature verification you're used to from the original electronic signature software, with some differences. These differences become apparent when a signature fails. When you have a failure on signature verification, after you are shown an error message, you should see the following window.



Check for data changes

Would you like to see a comparison of the data you are verifying and the original signed data to see the changes (if possible)?

WinSig has the ability to research a signature failure and display the changed data for the user as soon as the failure occurs. Clicking the "No" button here dismisses the window and returns control to CEFMS, which in turn displays the error you received. Clicking the "Yes" button will bring up a window similar to the one that follows.



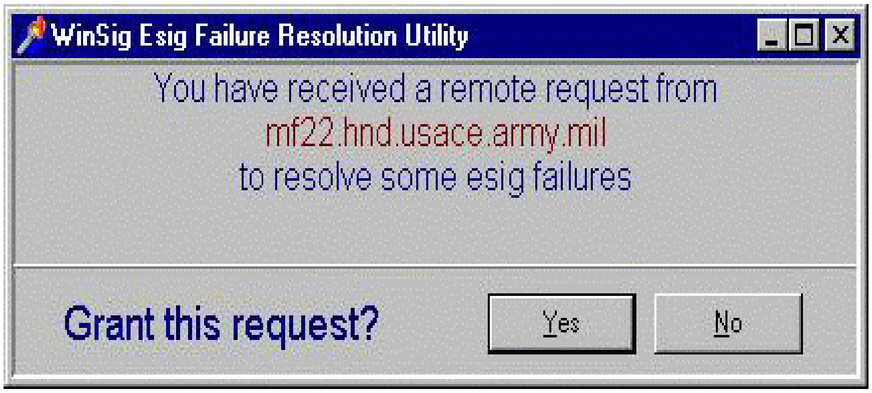
Electronic signature data changes

Originally signed by: FREDERICK ANDERSON

Date: Fri Jan 16 09:24:36 1998

Description	Original data	Current data
THE AMOUNT OF THE CHECK	2500	2001

As can be seen from the window, in this instance, the amount of a CEFMS check has been modified from 2500 to 2001. Failure resolution should be considerably easier now that WinSig can provide this information to the user. Failure resolution is only available if the user signs the document using WinSig and if the log files have not been archived to tape. If the changed data is now incorrect, the site's CEFMS Point of Contact must be contacted in order to get the data changed to the proper value. In most cases, this will require the site to enter a CEFMS customer inquiry.   After the user who originally signed the document determines that the data is correct, that user may resign the data.



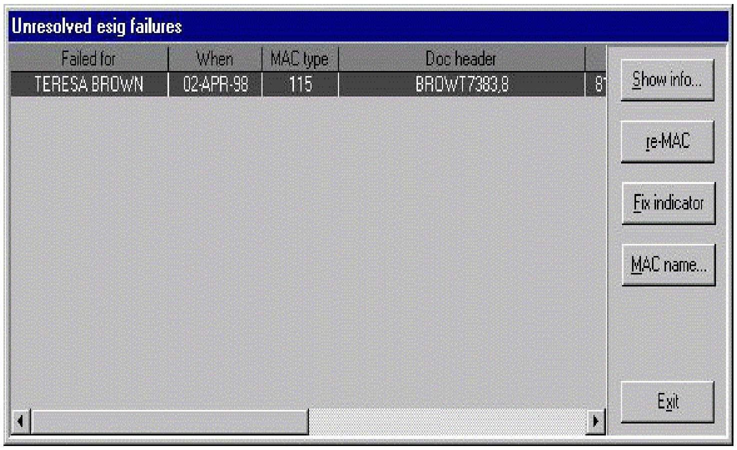
You have received a remote request from
mf22.hnd.usace.army.mil
to resolve some esig failures

Grant this request?

The WinSig system provides a simple mechanism to re-sign documents provided that the data is accurate. In order to have a document re-signed, the user who originally signed the document (the originating user's name can be seen in the window above) must select option 8, "RESOLVE ESIG FAILURES", from the CEFMS Electronic Signature Menu. Selecting this option to resolve an electronic signature failure will display a window like the following one below.

Please notice that everything in WinSig requires your acceptance. WinSig will not execute a command without your permission.

Clicking the “Yes” button will start the WinSig resolver, shown below.

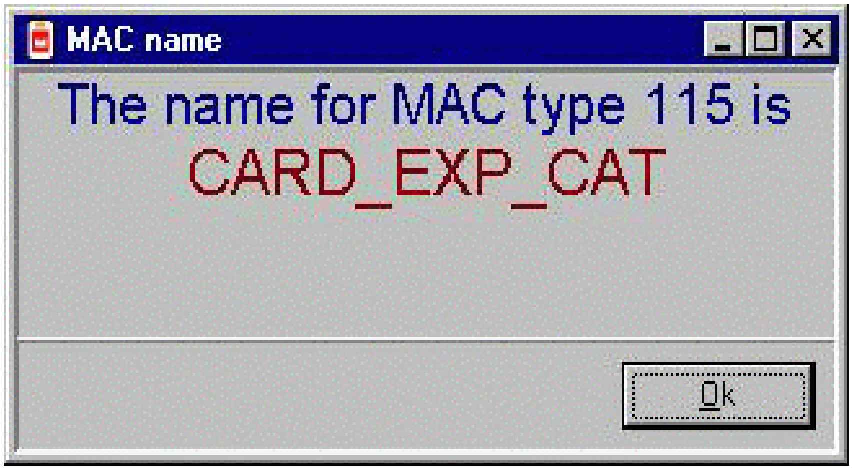


Unresolved esig failures

Failed for	When	MAC type	Doc header	
TERESA BROWN	02-APR-98	115	BROWT7383,8	8

The WinSig failure resolver will show every unresolved failure for signatures you have generated. Please notice that the resolver does not show failures you have gotten; it shows failures other people have gotten on signatures generated by you. Clicking the “Show Info” button will show you a field by field comparison of the data you signed and the data that failed, so you can note changes and determine if they are valid. Clicking the “re-MAC” button will generate a new electronic signature on the failed data, so make sure the failed data is now valid before you do this. If the original user is no longer available to sign the document, option 9 - DATA MANAGER ESIG FAILURE RESOLUTION on the CEFMS electronic signature menu is available for a data manager to resolve an esig failure for any user.

The fix indicator button will set the transaction selected to resolved. This will be used when there are multiple esig failures for one document or if the data has been corrected so the remac is no longer required. The MAC Name button will display the MAC Name for the transaction in a screen like the one below.



MAC name

The name for MAC type 115 is
CARD_EXP_CAT

All screen shots in this guide are from the beta version of WinSig and are prone to be slightly different from the final release.

1.6 ReMAC.

A CEFMS menu option has replaced the ReMAC program. Previously, there was a ReMAC program executed from the /usr/tools/cefms/data UNIX directory. However, this program is no longer available and has been replaced with the ReMAC Utility option in CEFMS.

To access the CEFMS ReMAC Utility option, choose the ReMAC Utility from the Corps of Engineers Electronic Signature Menu.

1.7 Archive of ESIG Log Files.

Option ten (10) on the Electronic Signature Menu will allow a database manager to export esig log records older than ninety (90) days. Records are exported to $CEFMSDATA directory. These records are then deleted from the database.

1.8 Error Messages.

Users may encounter error conditions when executing WinSig. Errors 1-63 are errors from the Litronic Argus/300 and could indicate a problem with a particular smartcard, smartcard reader, or cryptographic module. Exceptions to this are errors 22, 24-26, 37, 39-42, 47, 58, and 60.
The following is a general list of error codes and messages to aid in the diagnosis of those conditions.

-11	Cannot write data to network connection
-10	Cannot read data from network connection
-9	Cannot determine remote host name
-8	Cannot accept remote connection
-7	Cannot listen for remote connection, out of system resources
-6	Cannot determine listening port for remote connection
-5	Cannot perform network bind on created connection
-4	Cannot connect to remote host
-3	Cannot create remote network connection
-2	Invalid remote host name specified

0	Success; no error
1	No cryptographic module present in PC
2	Internal RAM test failure in cryptographic module
3	ACP timer failure in cryptographic module
4	External RAM test failure in cryptographic module
5	ACP checksum error
6	ACP logic error
7	ACP watchdog error
8	ACP tampering error
9	DES s-box error
10	Zeroing failure
11	RNG seed failure
12	RNG failure
13	SA logon failed
14	User logon failed
15	No response from PC
16	Get host name
20	Bad hash
21	Invalid parameter
22	Smartcard hard lock (too many incorrect passwords entered)
23	Bad authentication vector on smartcard
24	Invalid password entered
25	Key already in use (i.e. log off the SA card before you try dSO)
26	Key cache full
27	Invalid key length
28	Bad internal counter
29	Failure to XOR keys
30	Key parity error
31	Attribute lock
32	Bad attribute
33	Key not found
34	Bad algorithm
35	Bad mode
36	ACP state error
37	Invalid password length (password must be exactly eight))characters)
38	Key checkword failure

39 Unauthorized command attempted (generally, exiting CEFMS and restarting your system will resolve this error)

40 Bad user type (i.e., it asked for an SA card, and you used a user or

41 No SA logged on

42 Same user logged in twice (you used your card as the SA card, and now you’re trying to use it as a user card)

43 Bad UID from smartcard

44 Bad DES chain

45 Bad DES feedback

46 ATR failed

47 No smartcard in reader

48 Smartcard I/O error

49 Smartcard reset

50 Smartcard type unsupported

51 No user logged in

52 Bad DES header

53 Smartcard command error

54 Smartcard not initialized

55 Smartcard has no authentication vector

56 Smartcard has no UID

57 No key on smartcard

58 Too many users logged into cryptographic module

59 Bad ACC sequence sent

60 MAC on header data failed, data may have been illegally changed

61 Bad length

62 Bad count

63 Bad key

64 User logon voluntarily terminated

65 SA logon voluntarily terminated

66 User logoff voluntarily terminated

67 SA logoff voluntarily terminated

68 dSO1 logon voluntarily terminated

69 dSO1 logoff voluntarily terminated

70 dSO2 logon voluntarily terminated

71 dSO2 logoff voluntarily terminated

72 No KTC info provided

73	Cryptographic module setup failed
74	Data integrity failed, data may have been illegally changed (same as error 21 in previous system)
75	Cannot read smartcard serial number
76	Cannot communicate with KTC
77	Smartcard remove cancelled
78	Invalid operation
79	User card has soft lock
80	Cannot determine user’s IP address
81	User not known to registry
82	No files to transfer
83	Grant denied
84	File transfer aborted
85	Send cancelled
86	Receive cancelled
87	Cannot print
88	Print cancelled
89	Resolve cancelled
90	Cannot resolve
91	Log message failed
92	Esig setup failed
94	Cannot open connection
95	Esig ISR not loaded
101	Signature creation refused by user
102	User wants to see data changes in a signature failure
103	User cancelled action
128	Originating user MAC’d after deactivation date
129	Originating user MAC’d after lost date
130	Originating SA MAC’d after deactivation date
131	Originating SA MAC’d after lost date
132	Current user MAC’d after deactivation date
133	Current user MAC’d after lost date
134	Current SA MAC’d after deactivation date
135	Current SA MAC’d after lost date
138	Current SA MAC’d before activation

139	Current user MAC’d before activation
140	Originating SA MAC’d before activation
141	Originating user MAC’d before activation
155	Card record MAC failed
156	Can’t get a SAD
157	Accept failed
158	Read failed
159	SO not logged in
160	No data to MAC
161	Data has not been electronically signed (esig not mandatory)
162	User not logged in (esig not mandatory)
163	Data has not been electronically signed (esig mandatory)
164	User not logged in (esig mandatory)
165	DSO1 logon failed
166	DSO2 logon failed
225	Smartcard not available for use
226	Smartcard already active at KTC
227	Smartcard cryptoperiod has expired
228	Current user’s cryptoperiod has expired
229	Current SA’s cryptoperiod has expired
230	Originating user’s cryptoperiod has expired
231	Originating SA’s cryptoperiod has expired
234	Originating SA smartcard not active at KTC
235	Originating user smartcard not active at KTC
236	Current SA smartcard not active at KTC
237	Current user smartcard not active at KTC
238	No counter for this site exists at KTC
239	Counter in CEFMS out of sync with KTC counter
240	User logon voluntarily terminated
241	Card already in data base
242	Cannot open card DB
243	Originating SA smartcard MAC failed at KTC
244	Originating user smartcard MAC failed at KTC
245	Current SA smartcard MAC failed at KTC
246	User pressed Invalid key

247	Smartcard logging cancelled
248	Current user smartcard MAC failed at KTC
249	Card activities disabled by CSOS
250	Already has an active card
251	Oracle error - watch specific message for details
252	RS card not active
254	Unknown command
255	Unknown command sent to WinSig
999	Unknown error